**Теорема.** *Если $x_1$ и $x_2$ не сравнимы, то соответствующие идеалы $\mathcal{I}_{x_2}$ и $\mathcal{I}_{x_1}$ различны. Если $x_1 \prec x_2$, то $\mathcal{I}_{x_2} \subseteq \mathcal{I}_{x_1}$.*

ЛИТЕРАТУРА

1. Кузнецова А. Ю. *Об одном классе $C^*$-алгебр, порождённых счётным семейством частичных изометрий* // Изв. НАН Армении. Матем. – 2010. – Т. 45 (6). – С. 51–62.

2. Кузнецова А. Ю., Патрин Е. В. *Об одном классе $C^*$-алгебр, порождённых частичными изометриями и мультипликаторами* // Изв. вузов. Матем. – 2012. – Т. 56 (6). – С. 44–55.

**К. А. Петухова**

*Казанский (Приволжский) федеральный университет,*
*ksenypet@mail.ru*

## ОБ АНАЛОГЕ ФУНКЦИИ ЭЙЛЕРА ДЛЯ ИДЕАЛОВ ДЕДЕКИНДОВЫХ КОЛЕЦ

В работе [1] был предложен аналог криптографического алгоритма RSA, в котором вместо натуральных чисел используются идеалы дедекиндовых колец. Одно из условий, которое необходимо наложить на дедекиндово кольцо $R$, – требование, чтобы для каждого максимального идеала $\mathfrak{M}$ поле $R/\mathfrak{M}$ было конечным (в дальнейшем это условие будет всюду подразумеваться). Тогда можно определить аналог функции Эйлера, который играет существенную роль в алгоритме RSA из [1], по формуле $\varphi_R(\mathfrak{A}) = |\mathrm{U}(\mathrm{R}/\mathfrak{A})|$, где $\mathfrak{A}$ – произвольный идеал $R$, U означает группу обратимых элементов кольца $R$.

В данной заметке приводится более подробная информация об этой функции. Из формулы (5) на с. 13 книги [2] следует

**Лемма 1.** *При условии, что поле $R/\mathfrak{M}$ конечно для всех максимальных идеалов $\mathfrak{M}$, кольца $R/\mathfrak{A}$ конечны для любых идеалов $\mathfrak{A}$. Это означает, что функция $\varphi_R(\mathfrak{A})$ определена для любых идеалов.*

В [1] был использован следующий аналог теоремы Эйлера:

**Теорема 1.** *Пусть $\mathfrak{M}$ – максимальный идеал, $a \notin \mathfrak{M}$, и $Ra + \mathfrak{M} = R$. Тогда $a^{\varphi_R(\mathfrak{M})} \equiv 1 \pmod{\mathfrak{M}}$.*

Обозначим через $\nu(\mathfrak{A})$ мощность конечного кольца $R/\mathfrak{A}$. Основным результатом заметки является следующая

**Теорема 2.** *Пусть $\mathfrak{M}$ – максимальный идеал $R$, $k > 0$ – натуральное число. Тогда*

$$\varphi_R(\mathfrak{M}^k) = \nu(\mathfrak{M})^{k+1} - \nu(\mathfrak{M})^k. \tag{1}$$

Частный случай формулы (1) доказан в книге [3] (теорема 2 на с. 202), но лишь для главных идеалов в областях целостности, каждое факторкольцо которых по главному идеалу конечно. В работе [4], на которую нет ссылки в [3], явно вычислены функции $\nu$ и $\varphi_R$ для идеалов кольца целых гауссовых чисел $R = \mathbb{Z}[i]$ (это область главных идеалов).

В нашем докладе будут приведены примеры вычислений функции $\varphi_R$ для некоторых других колец целых алгебраических чисел.

Работа выполнена за счет средств субсидии, выделенной Казанскому (Приволжскому) федеральному университету для выполнения проектной части государственного задания в сфере научной деятельности (проект № 2045).

ЛИТЕРАТУРА

1. Тронин С. Н., Петухова К. А. *RSA cryptosystem for Dedekind rings* // Мат. конф. "Алгебра и математическая логика: теория и приложения" (г. Казань, 2–6 июня 2014 г.) и сопутствующей молодежной летней школы "Вычислимость и вычислимые структуры". – Казань: Изд-во Казан. ун-та, 2014. – С. 148–149.

2. Swinnerton-Dyer H. P. F. *A brief guide to algebraic number theory.* – Cambridge University press, 2001. – 145 p.

3. Родосский К. А. *Алгоритм Евклида.* – М.: Наука, 1988. – 240 с.

4. Cross J. T. *The Euler $\varphi$-function in the Gaussian integers* // The American Mathematical Monthly. – 1983. – V. 90. – No 80. – P. 518–528.

**В. Н. Попов, Е. А. Смоленская, И. В. Тестова**

*Северный (Арктический) федеральный университет им. М. В. Ломоносова,*

*v.popov@narfu.ru, e.smoltnskaya@narfu.ru, testovairina@mail.ru*

## МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ОБТЕКАНИЯ РАЗРЕЖЕННЫМ ГАЗОМ НЕОДНОРОДНО НАГРЕТОЙ ПЛОСКОЙ ПОВЕРХНОСТИ

Рассматривается задача об обтекании разреженным газом неоднородно нагретой плоской поверхности. Показано, что с использованием линеаризованной ЭС (эллипсоидально-статистической) модели кинетического уравнения Больцмана в качестве основного уравнения, описывающего кинетику процесса, и модели зеркально-диффузного отражения Максвелла